SPR 8739.1 Rev. A
July 2010

National Aeronautics and
Space Administration

John C. Stennis Space Center
Stennis Space Center, MS
39529-6000

COMPLIANCE IS MANDATORY

John C. Stennis Space Center
Software Assurance Procedural Requirements

Stennis	SPR 8739.1		A
Procedural Requirements	Number		Rev.
	Effective Date: July 15, 2010		
	Expiration Date: July 15, 2015		
			Page 2 of 17

Responsible Office: Office of Safety and Mission Assurance

SUBJECT: Software Assurance Procedural Requirements

Document History Log

Status/Change/ Revision	Change Date	Originator/Phone	Description
Basic	11/02/2007	Charles Fallo/8-2553	Initial Release
Rev A	06/09/10	Charles Fallo/8-2553	Updated Center Director signature block. Added section 2.9.h

Stennis Procedural Requirements	SPR 8739.1		A
	Number		Rev.
	Effective Date: July 15, 2010		
	Expiration Date: July 15, 2015		
			Page 3 of 17
Responsible Office: Office of Safety and Mission Assurance			
SUBJECT: Software Assurance Procedural Requirements			

Table of Contents

Stennis		SPR 8739.1		A
Procedural Requirements		Number		Rev.
		Effective Date: July 15, 2010		
		Expiration Date: July 15, 2015		
				Page 4 of 17
Responsible Office: Office of Safety and Mission Assurance				
SUBJECT: Software Assurance Procedural Requirements				

FIGURES

Stennis Procedural Requirements	SPR 8739.1		A
	Number		Rev.
	Effective Date: July 15, 2010		
	Expiration Date: July 15, 2015		
			Page 5 of 17

Responsible Office: Office of Safety and Mission Assurance

SUBJECT: Software Assurance Procedural Requirements

PREFACE

P.1   PURPOSE

a. This Stennis Procedural Requirement (SPR) specifies the requirements for Software Assurance (SA) and Software Safety (SS) for NASA Stennis Space Center (SSC) projects, programs, facilities, and activities. The NASA NPR 7150.2, Software Engineering Requirements document also provides guidance for NASA SA and SS activities.

b. This SPR establishes the procedures necessary for SSC to comply with the requirements for SA and SS for software developed or acquired by NASA SSC, including open source, Government off-the-Shelf (GOTS) software, Modified off-the-Shelf (MOTS) software, and Commercial off-the-Shelf (COTS) software, when included in a NASA system.

c. Requirements in this SPR implement SSC software management practices to be used in conjunction with the following two NASA Agency-wide standards:

- NASA-STD-8739.8, Software Assurance Standard that describes the processes and procedures for analyzing and applying appropriate software assurance techniques and methods to software, and
- NASA-STD-8719.13, Software Safety Standard that describes the activities necessary to ensure that safety is designed into the software that is acquired or developed by NASA. It specifies the software safety activities, data, and documentation necessary for the acquisition or development of software in a safety-critical system.

d. A blend of the software requirements specified in the SA and SS standards is used to ensure that all software requirements involving the overall management, engineering, and assurance activities are integrally satisfied. These standards must be used by software engineers, managers, assurance engineers, and safety practitioners to assess software systems for the software's contribution to safety and quality.

P.2   APPLICABILITY

a. This SSC Procedural Requirement is applicable to all NASA SSC personnel and to NASA SSC contractors to the extent specified or referenced in their respective contracts.

b. The requirements of this document are applicable whenever NASA is either the acquirer or provider of software, and to the extent specified in the contract or other agreement such as Memorandum of Agreement/Understanding.

c. According to NASA-STD-8739.8, Software Assurance requirements for Classes F, G, and H are designated by the Office of the Chief Information Officer (OCIO). As such, at this time SA is only performed on these classes upon request or as designated by the OCIO.

Stennis Procedural Requirements	SPR 8739.1	A
	Number	*Rev.*
	Effective Date: July 15, 2010	
	Expiration Date: July 15, 2015	
		Page 6 of 17

Responsible Office: Office of Safety and Mission Assurance

SUBJECT: Software Assurance Procedural Requirements

d. Class descriptions as provided in NPR 7150.2 are:

Class A - Human Rated Software Systems
Class B - Non-Human Space Rated Software Systems
Class C - Mission Support Software
Class D - Analysis and Distribution Software
Class E - Development Support Software
Class F - General Purpose Computing Software (Multi-Center or Multi-Program/Project)
Class G – General Purpose Computing Software (Single-Center or Project)
Class H - General Purpose Desktop Software

e. The focus of this SPR is software belonging to software Classes A-E.

f. The requirements are applicable to all software and firmware developed and acquired by, or for, NASA SSC, including GOTS, MOTS, and COTS software when included in a NASA SSC system. Applicable NASA SSC systems include, but are not necessarily limited to, facilities and projects including the Test Complex Facility, Hazardous Gas Detection & Warning System, High Pressure Gas Facility, High Pressure Industrial Water Plant, Applied Science Projects, Test Complex Management Systems (Rocketdyne Automated Management System (RAMS), Document Data Management System (DDMS), and Master Work Control), test beds, ground support systems, other facility systems, and software projects that support or perform NASA SSC specific missions.

g. The SA requirements apply to the entire software life cycle of the software developed or modified, either acquired or provided, for NASA SSC as outlined in the NASA SA Standard.

P.3 AUTHORITY

a. NPD 2820.1, NASA Software Policy.
b. NPR 7150.2, NASA Software Engineering Requirements.

P.4 APPLICABLE DOCUMENTS

All references are assumed to be the latest version unless otherwise specified.

a. NPR 1441.1, NASA Records Retention Schedules.
b. NPR 7120.5, NASA Program and Project Management Processes and Requirements.
c. NPR 7150.2, NASA Software Engineering Requirements.
d. NPR 8715.3, NASA General Safety Program Requirements.
e. NASA-STD-8719.13, Software Safety Standard.
f. NASA-STD-8739.8, Software Assurance Standard.
g. SPR 1440.1, Records Management Program Requirements.

Responsible Office: Office of Safety and Mission Assurance

SUBJECT: Software Assurance Procedural Requirements

h. SSTD-8070-0007-CONFIG, Variance and Alternate Standard Requests.
i. SOI-8000-0001, SSC Project Directorate Risk Management Plan.
j. SOI-8080-0008, Documentation and Configuration Control of Test Critical Software.
k. SSLP-3410-0001, Training.
l. SCWI-3410-0002, Training and Development Plan.
m. SSP-8715-0001, SSC Safety and Health Handbook

P.5   MEASUREMENT AND VERIFICATION

Compliance with this procedure will be monitored through the Stennis Space Center Management System (SMS) and Office of Safety and Mission Assurance by objective evidence, such as Training records, Functional S&MA Organization Chart SA Role Assignment provided, Annual Operating Agreement (AOA), S&MA Work Instructions generated, and SA Task Developed Products/Documents (reference Section 2.11).

P.6   CANCELLATION

None

Patrick E. Scheuermann
Director

DISTRIBUTION
Approved for public release via NODIS; distribution is unlimited.

Stennis Procedural Requirements	SPR 8739.1	A
	Number	*Rev.*
	Effective Date: July 15, 2010	
	Expiration Date: July 15, 2015	
		Page 8 of 17

Responsible Office: Office of Safety and Mission Assurance

SUBJECT: Software Assurance Procedural Requirements

CHAPTER 1. ORGANIZATION

1.1   Organizational Structure

Successful compliance and management of all NASA SSC SA activities associated with projects that use software requires the involvement at many levels of the organization. Figure 1 provides a diagram that shows how the various NASA SSC personnel coordinate roles to assure SA reporting activities are implemented to comply with the SA and SS standards.
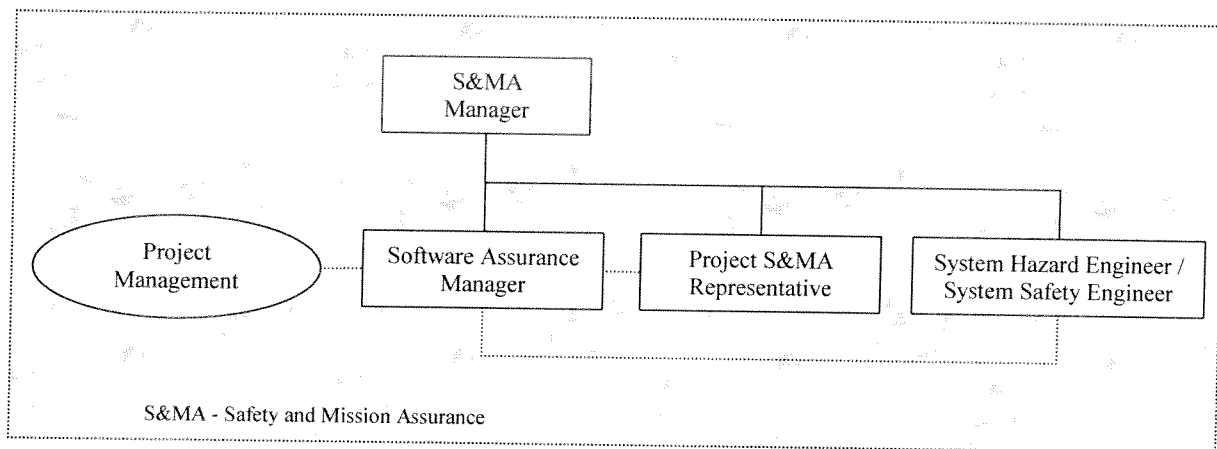

Figure 1 Organizational Chart for Management of Software Assurance Reporting Activities

1.2   Roles and Responsibilities

1.2.1   Project Management

Project Management is responsible for:

a. Ensuring compliance with the NPD 2820.1, NASA Software Policy, NPR 7150.2, NASA Software Engineering Requirements.

b. Ensuring software developing organization(s) support the development of a hazard analysis (HA) which includes software, e.g., SOI-8000-0001, SSC Project Directorate Risk Management Plan, SOI-8080-0008, Documentation and Configuration Control of Test Critical Software.

c. Approving the program or project's assurance and safety effort as documented in the Program (Project) Software Assurance Plan.

d. Ensuring the safety requirements of NASA-STD-8719.13, Software Safety, are implemented by the project when a project is determined to have safety critical software.

Stennis Procedural Requirements	SPR 8739.1	A
	Number	Rev.
	Effective Date: July 15, 2010	
	Expiration Date: July 15, 2015	
		Page 9 of 17

Responsible Office: Office of Safety and Mission Assurance

SUBJECT: Software Assurance Procedural Requirements

1.2.2 Safety and Mission Assurance (S&MA) Manager

S&MA is independent from the project and assures software assurance activities and the results. S&MA is responsible for:

a. Assuring that SSC complies with the NASA-STD-8739.8, Software Assurance Standard, and the NASA-STD-8719.13, Software Safety Standard.

b. Providing resources for S&MA's SA Manager, Project Representative, and System Hazard Engineer / System Safety Engineer assigned to projects at SSC for quality, safety, reliability and mission assurance oversight.

c. Identifying a SA Manager within S&MA who is responsible for implementing the SA and SS standards.

1.2.3 Software Assurance Manager

The SA Manager is responsible for:

a. Directing and managing the SA procedural requirements, along with conducting and documenting periodic reviews, audits, and assessments of the development processes and products. Depending on the software's operational environment and the criticality of operation, the SA Manager is responsible for ensuring that any changes to the software or software work enhancements have been addressed and approved based on the outcomes of the periodic reviews, audits and/or assessments.

b. Preparing the Program Software Assurance Plan (PSAP) or a respective Project Software Assurance Plan for software classes A–D specific software assurance process activities.

c. Conducting a Preliminary Hazard Analysis to determine if software is Software Safety Critical.

d. Completing the Software Assurance Classification Report early in the process, i.e., System Requirements Review (SRR).

e. Providing checklists to assess compliance to the NASA SA Standard and NASA SS Standard (for software safety systems), according to the PSAP.

f. Reporting software assurance activity status to appropriate levels of management.

g. Assuring that software engineering and management prepare, approve, and execute a retirement plan, prior to the retirement or disposition of software products.

Stennis	SPR 8739.1		A
Procedural Requirements	*Number*		*Rev.*
	Effective Date: July 15, 2010	
	Expiration Date: July 15, 2015	
		Page 10 of 17

Responsible Office: Office of Safety and Mission Assurance

SUBJECT: Software Assurance Procedural Requirements

h. Ensuring software retirement plan includes archival and eventual disposal of software assurance records and documents created over the program/project in accordance with the requirements of SPR 1440.1, Records Management Program Requirements

i. Assuring SSC software documentation requirements follow direction as specified in NPR 7150.2 Chapter 5: Software Documentation Requirements.

1.2.4   Project S&MA Representatives

The Project S&MA Representatives are responsible for:

a. Performing software assurance and software safety functions for S&MA on their assigned projects through a checklist for inspection, witness, surveillance, and verification of artifacts and processes are incompliance to the standards within the Project.

b. Coordinating with the respective project's team, to ensure that all software assurance and software safety (safety, quality, reliability, verification and validation) requirements are satisfied.

c. Verifying compliance to the NASA SA Standard and NASA SS Standard. This support is applied to assigned projects requiring software assurance and software safety.

d. Assuring NASA and SSC software policies and standards, applicable to a project, are followed properly.

e. Assuring that reported issues, problems and risks are reported, recorded, addressed, and tracked to closure.

f. Assuring that all unresolved SA issues are elevated to the appropriate governing authority, as provided in NPR 7150.2. Figure 2 depicts the "directional steps" for the governing lines of authority for resolving SSC SA issues.

Stennis	SPR 8739.1		A
Procedural Requirements	Number		Rev.
	Effective Date: July 15, 2010		
	Expiration Date: July 15, 2015		
			Page 11 of 17

Responsible Office: Office of Safety and Mission Assurance

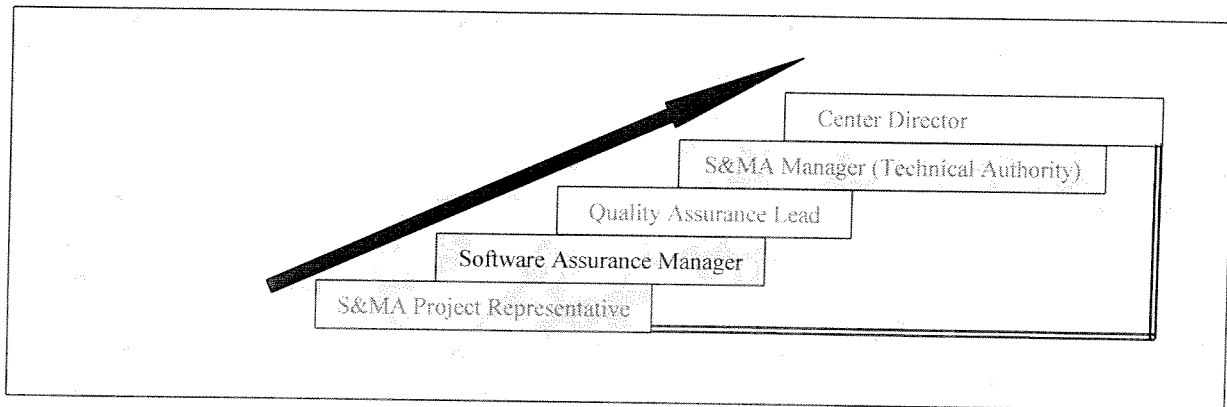SUBJECT: Software Assurance Procedural Requirements

Figure 2 Governing Lines of Authority for Resolving SSC SA Issues

1.2.5   System Hazard Engineer/System Safety Engineer

The System Hazard Engineer is responsible for:

a. Identifying the hazards within a system, including software, and performing the appropriate system Preliminary Hazard Analysis (PHA) to determine the software's safety-critical state.

b. Coordinating with other safety and software engineers and project management to determine the software's safety contribution, the controls, design features, verifications, and requirements needed to assure safe software in a safe system.

c. Identifying controls to mitigate inherent risks for software within a system.

d. Performing PHA, HA, and System Hazard Analysis (SHA) according to NPR 8715.3, SSP-8715-0001 SSC Safety and Health Handbook.

1.2.6   Contractor Safety and Mission Assurance (SMA)

a.   This document applies to contractors SMA organization as specified in their contract.

b.   Contractor SMA deliverable products shall be specified by contract.

1.2.7   Software Acquirer

a. The Software Acquirer (or customer) is the entity or individuals who specifies the requirements for the software and accepts the resulting software products. These are generally NASA SSC civil servants or Prime Contractor personnel.

Stennis	SPR 8739.1		A
Procedural Requirements	*Number*		*Rev.*
	Effective Date: July 15, 2010		
	Expiration Date: July 15, 2015		
			Page 12 of 17

Responsible Office: Office of Safety and Mission Assurance

SUBJECT: Software Assurance Procedural Requirements

b. The Software Acquirer is responsible for addressing requirements as specified in the NASA SA Standard section 5.0 or to the extent specified in the contract or other agreement such as Memorandum of Agreement/Understanding. Specifically, the Software Acquirer is responsible for specifying the SA requirements for the entire life cycle of the product.

1.2.8   Software Provider

a. The Software Provider (or supplier) refers to the entities or individuals that design, develop, implement, test, operate, and maintain the software products.

b. The Software Provider is responsible for addressing requirements as specified in the NASA SA Standard section 6.0 or to the extent specified in the contract or other agreement such as Memorandum of Agreement/Understanding.

c. The Software Provider is responsible for ensuring that acquisitions internal to NASA will follow the NASA SA standard.

1.2.9 SSC Independent Verification and Validation (IV&V) Liaison

The S&MA IV&V Liaison is responsible for independent review of the SSC's software inventory, serving as Point of Contact (POC) for the Center if IV&V is required, and creating an IV&V plan if IV&V is selected for a project.

Stennis Procedural Requirements	SPR 8739.1	A
	Number	*Rev.*
	Effective Date: July 15, 2010	
	Expiration Date: July 15, 2015	
		Page 13 of 17

Responsible Office: Office of Safety and Mission Assurance

SUBJECT: Software Assurance Procedural Requirements

CHAPTER 2. SOFTWARE ASSURANCE PROCESS

2.1 Definition

The NASA SSC SA process is a planned and systematic set of activities to ensure the conformance of software life cycle processes and products to requirements, standards, and procedures. SA assures that the software and its related products meet their specified requirements, conform to standards and regulations, are consistent, complete, correct, safe, secure and reliable as warranted for the system and operating environment, and satisfy customer needs.

2.2 Implementation

a. This directive shall apply to new contracts and subcontracts which develop software for NASA systems and referenced within those contracts.

b. The procuring SSC NASA Directorate shall comply with this directive and, work with the Safety and Mission Assurance SSC Software Assurance Manager, to make a conscious, documented decision as to how best to apply these requirements to current contracts and ongoing projects.

2.3 Training

a. All personnel who perform SA activities shall be trained and possess the proper skills for the SA endeavors. Refer to SSLP-3410-0001,Training, and SCWI-3410-0002, Training and Development Plan.

b. Training requirements will be tailored according to needs. Types of training are listed but not limited to items shown below.

- Software Assurance
- Software Safety
- Software System Safety

c. The Program Software Assurance Plan shall identify training requirements necessary to meet the needs for implementing the Software Assurance Activity.

d. Appropriate records of training shall be maintained, i.e., in the Training Certification Record System (TCRSII).

Stennis Procedural Requirements	SPR 8739.1	A
	Number	Rev.
	Effective Date: July 15, 2010	
	Expiration Date: July 15, 2015	
		Page 14 of 17

Responsible Office: Office of Safety and Mission Assurance

SUBJECT: Software Assurance Procedural Requirements

2.4 NASA SSC Software Life Cycle Management Requirement

a. The NASA SSC software life cycle management requirements conform to applicable sections of NASA NPR 7120.5, Program and Project Management Processes and Requirements. Certain phases determine which activities will be performed.

b. Management of SSC SA activities shall be implemented at the project formulation stage.

c. The SSC SA requirements shall be assured for the duration of the software's life cycle which includes acquisition, supply, development, operation, and maintenance.

d. The Program / Project Software Assurance Plan shall address the following key software assurance disciplines:

- Software Quality (Assurance, Control and Engineering)
- Safety
- Reliability
- Verification and Validation (V&V)
- Independent Verification and Validation (IV&V)

e. The NASA-STD-8739.8, Software Assurance Standard shall be referenced to address each of the software life cycle disciplines.

2.5 Tailoring, Deviations, and Waivers

a. Implementation of the SSC SA requirements may be tailored based on the software classification as well as size, complexity, criticality, and risk.

b. SSC SA tailoring shall be performed in accordance with the NASA SA Standard and NPR 7150.2.

c. SSC SA waivers and/or variances shall be processed in accordance with the NASA Safety Manual NPR 8715.3, the NASA SA Standard, and the governing Technical Authority (TA) per Variance and Alternate Standard Requests, SSTD-8070-0007-CONFIG.

2.6 Functional SA Role Assignment and Resources

a. Prior to performing any SA Process activities, S&MA shall assure that all functional SA roles are assigned and resources provided as described in Section 1.2 above.

b. Functional SA roles shall include the respective S&MA Project Representative, the SA Manager, and the System Hazard Engineer/System Safety Engineer.

Stennis Procedural Requirements	SPR 8739.1		A
	Number		Rev.
	Effective Date: July 15, 2010		
	Expiration Date: July 15, 2015		
			Page 15 of 17

Responsible Office: Office of Safety and Mission Assurance

SUBJECT: Software Assurance Procedural Requirements

2.7   Software Assurance Classification Assessment

a. The Software Engineer, System Engineer, Project Manager, and Software Assurance Manager shall perform and participate in a Software Assurance Classification Assessment of the software and software components for a project, according to the NASA SA standard, to evaluate and thereby, classify the software.

b. The NASA SSC Software Assurance Classification Report (SSC Form SSC-809) shall be placed under configuration control by the appropriate authorizing board. The appropriate board may be civil servant or contractor, as necessary, to maintain configuration control.

c. The SA Classification Report shall be used to prioritize SA level of efforts for SSC software.

2.8   Software Safety Criticality

a. A PHA, HA, and SHA shall be conducted per NPR 8715.3 and SSP-8715-0001 SSC Safety and Health Handbook by the organization developing the software. The PHA is used to determine if the software is safety critical and to establish the Risk Assessment Code (RAC).

b. The SA Manager & S&MA Project Representative shall participate in the review of the system software Preliminary Hazard Analysis / Hazard Analysis report.

c. Software shall be analyzed by the System Hazard Engineer / System Safety Engineer and SA Manager to determine if software has a potential for causing a hazard, or is part of a system that controls, monitors or mitigates a hazard.

d. The PHA / HA system software safety analysis shall adhere to the NASA-STD-8719.13, Software Safety Standard.

e. If software is found to be safety critical, the SA Manager and Project Management shall comply with the requirements of NASA-STD-8719.13.

f. During operational use of the software safety critical software, all discrepancies, changes and reconfigurations shall be reviewed and analyzed for system safety by S&MA's Project Representative.

g. If adverse system safety effects exist, the HA shall be updated.

2.9   Program Software Assurance Plan

a. Each program shall develop a PSAP for software belonging to Classes A-D that addresses all software development and maintenance activities. For smaller projects, this may be incorporated in another project planning document or in a Project Software Assurance Plan.

Stennis Procedural Requirements	SPR 8739.1	A
	Number	Rev.
	Effective Date: July 15, 2010	
	Expiration Date: July 15, 2015	
		Page 16 of 17

Responsible Office: Office of Safety and Mission Assurance

SUBJECT: Software Assurance Procedural Requirements

b. Planning documents shall conform to NASA-STD-8739.8, SA Standard for SA Plans.

c. The plan shall be developed and tailored to meet the development processes and procedures used by the program / project.

d. Each program / project shall follow their respective PSAP.

e. The PSAP shall detail the procedures, reviews, and audits required to accomplish software assurance.

f. S&MA shall obtain concurrence with project management as to the extent and responsibilities for the project's assurance and safety effort as documented in the Program or Project Software Assurance Plan.

g. The PSAP shall describe the metrics required for collection and reporting the software assurance activities in accordance with the SA and SS Standards.

h. For Class C software and higher, the PSAP shall require reviewing the program and project software metric report to provide insight into the software development team.

2.10   Software Assurance Task Review Process

During development, implementation, and operation, the SA task activities shall be monitored by the SA Manager, and/or the Project S&MA Representatives to ensure that SA practices remain in place and are being followed accordingly.

2.11   Software Assurance Task Developed Products/Documents

a. The products and records developed by the SA activities shall, at a minimum, include the following:

- NASA SSC SA Classification Report
- Specific Project SA Preliminary Hazard Analysis (PHA) Report
- Specific Program Software Assurance Plan
- Software Assurance Checklist
- Process/Product Audit Reports
- SA Status Reports

b. Records shall be maintained in accordance with NPR 1441.1, NASA Records Retention Schedules and SPR 1440.1, SSC Records Management Program Requirements.

Stennis	SPR 8739.1		A
Procedural Requirements	*Number*		*Rev.*
	Effective Date: July 15, 2010		
	Expiration Date: July 15, 2015		
			Page 17 of 17

Responsible Office: Office of Safety and Mission Assurance

SUBJECT: Software Assurance Procedural Requirements

APPENDIX A – Abbreviations and Acronyms

AOA	Annual Operating Agreement
COTS	Commercial-off-the-Shelf software
DDMS	Document Data Management System
GOTS	Government-off-the-Shelf software
HA	Hazard Analysis
IV&V	Independent Verification & Validation
MOA	Memorandum of Agreement
MOTS	Modified-off-the-Shelf software
MOU	Memorandum of Understanding
NASA	National Aeronautical and Space Administration
NODIS	NASA Online Directives Information System
NPD	NASA Procedural Directive
NPR	NASA Procedural Requirement
OCIO	Office of the Chief Information Officer
S&MA	Safety and Mission Assurance
PHA	Preliminary Hazard Analysis
POC	Point-of-Contact
PSAP	Program Software Assurance Plan
QA	Quality Assurance
RAC	Risk Assessment Code
RAMS	Rocketdyne Automatic Management System
SA	Software Assurance
SHA	System Hazard Analysis
SMS	Stennis Space Center Management System
SPG	SSC Procedures and Guidelines
SPR	Stennis Procedural Requirement
SRR	System Requirements Review
SS	Software Safety
SSC	Stennis Space Center
STD	Standard
SWR	Stennis Work Request
TA	Technical Authority
TCRSII	Training Certification Record System
V&V	Verification & Validation